Inventory Delivery System (IDS), Release 1., Milestone 2/3, version 1.0
Privacy Impact Assessment

PIA Approval Date – Sept. 18, 2007

IDS System Overview

The Inventory Delivery System (IDS) is a rule-based, decision support system that will enhance existing compliance/collection systems of the IRS by directing tax-delinquent cases to the precise point in the collection process where they can be processed optimally. Future enhancements being developed for IDS are grouped in the project Consolidated Decision Analytics (CDA).

Description of System

The Inventory Delivery System (IDS) is a rule-based, decision support system that will enhance existing compliance/collection systems of the IRS by directing tax-delinquent cases to the precise point in the collection process where they can be processed optimally. Future enhancements being developed for IDS are grouped in the project Consolidated Decision Analytics (CDA). All application users are IRS Wage and Investment (W&I) and Small Business/Self Employed (SB/SE) employees. The user groups include, System Administrators, Headquarter Analysts, IDS Clerks, and IDS Managers. There will be approximately 250 authorized IDS/Consolidated Decision Analytics (CDA) users with 230 being address research users. The remaining 20 users will consist of analysts accessing rules within IDS/CDA. The batch analysis performed generates the data source once a week from the Taxpayer Information File (TIF) and Corporate Files Online (CFOL) and processes data extraction set-automatically. Data files are received daily via connection interface from TIF and CFOL. The IDS will:

- Analyze each case to determine if it is a suitable candidate for hands-on casework by Automated Collection System (ACS) call-site personnel and revenue officers in the Collection Field function(CFf).
- Perfect casework by using its research services to obtain missing taxpayer information needed for case resolution.
- Classify and direct perfected cases to the collection entity that is best suited to work particular types of inventory.
- Close cases and remove them from the active inventory when criteria for case distribution to collection units are not met.

The IDS consists of the following components:

- LOAD – The station where initial taxpayer case data is received from various sources.
- ROUTER – The station that distributes cases to and from the Address Research (ADR), Telephone Research (TNR), and Case Initialization (CASE INIT) stations.
- BYPASS – The station where business rules are applied to determine whether cases are closed, referred to other systems, or assigned to another IRS collection function or process.

To resolve the current limitations and deficiencies, the IDS enhancements are expected to:

- Incorporate technology that enables most of the business rule changes to be made by business analysts rather than programmers, reducing the need for time intensive programming changes.
- Improve the scoring of cases by using a more advanced scoring engine. IDS will send relevant internal IRS data to the solution's scoring engine. The engine will determine what external information is needed and contacts third-party vendors for the data. The engine will

evaluate the case based on the comprehensive compilation of internal and external information and passes back a score to IDS.

- Enable the treatment of cases on an entity basis. The solution will enable the system to score a case based on all modules so that the yield is more accurate. Routing rules will also be based on handling an entity rather than applying routing actions on individual modules.
- Expand its modeling capabilities to include all cases coming from the different BODs, not just SB/SE. All cases will be eligible to execute the same modeling and scoring functions available to SB/SE notice cases. The scores will allow the system to more accurately and efficiently route each case to the proper work streams.
- Expand the data set available to IDS. It will use existing internal data, newly available internal data, and newly available external data to gain a better perspective of each taxpayer so that better predictive indicators can label a case as low or high yield. This comprehensive data set will greatly enhance the efficiency and accuracy of scoring. The resulting scores will enable more discrete decisions on case routing and prioritization which are not possible under the current system.
- Modify low-level procedural steps to accommodate and improve individual case resolution decisions and high-level organization resource allocation decisions. For example, the system should be able to determine how to achieve optimum distribution of staffing between field, call site, and campus, and how to balance collection and compliance outcomes.

All Collection activities benefit from IDS processing but the only “users” of IDS are those who interface through the ADR system. ADR users are located in Undelivered Mail units located in each Campus.

System of Records Number(s) (SORN)

- Treasury/IRS 23.012 Offers in Compromise
- Treasury/IRS 26.016 Returns Compliance Program
- Treasury/IRS 26.019 Taxpayer Delinquency Account
- Treasury/IRS 26.020 Taxpayer Delinquency Investigation
- Treasury/IRS 26.022 Delinquency Prevention Programs
- Treasury/IRS 34.037 IRS Audit and Security Records System

Data in the System

1. Generally describe the information to be used in the system in each of the following categories: Taxpayer, Employee, and Other.

A. Taxpayer:

- Taxpayer income information
- Financial Information (Bank name and address, routing number, name of the account holder, account number, real estate, assets, wage and levy sources)
- Taxpayer Identification Number (TIN)
- Tax return information (filing status, tax year)
- Taxpayer address
- Taxpayer name
- Taxpayer telephone numbers

B. Employee:

- Employee name
- Employee Standard Employee Identification (SEID) number
- Employee Service Center location, status (active, furloughed, terminated, etc.),
- Employee role (manager, analyst, Customer Service Representative (CSR)), security officer, etc.),
- Permitted tasks

C. Other: None

D. Audit Trail Information: TINs, updated address and date, SEID, TIN Type, file source code (tells the type of account)

2. What are the sources of the information in the system?

Standardized Integrated Data Retrieval System Access (SIA), Automated Collection System (ACS), Address Research (ADR) Vendor, Telephone Number Research (TNR) Vendor, Integrated Collection System (ICS), Choicepoint (provides taxpayer addresses), United States Post Office (postal tracers including taxpayer address)

2.a. What IRS files and databases are used?

ADR Vendor: New address and telephone number
TNR Vendor: Telephone numbers
ACS: address and telephone information, tax period, TIN, TIN Type and file source and tax modules
SIA: Entity and tax modules
ICS-List of zip codes associated with the business unit employees working a particular case

2.b. What Federal Agencies are providing data for use in the system?

The United States Postal Service supplies IDS with postal tracers (provide address information)

2.c. What State and Local Agencies are providing data for use in the system?

State and Local Agencies are not providing data to IDS.

2.d. From what other third party sources will data be collected?

IDS currently receive third party data from Choicepoint.

2.e. What information will be collected from the taxpayer/employee?

Taxpayer:

- Taxpayer address
- Taxpayer telephone numbers

Employee:

- Employee name (first, middle initial, last)
- Employee role
- Employee SEID
- Managers SEID

3.a. How will the data collected from sources other than IRS records and the taxpayers be verified for accuracy?
IDS verifies address information received from Choicepoint by using an address-standardization COTS (Commercial Off-The-Shelf) product CODE1. A taxpayer signature is required and verifies the address before any update takes place.

IDS relies on the postal tracers providing taxpayer address information from the United States Postal Service to be accurate.

3.b. How will data be checked for completeness?
Currently, IDS performs internal testing of each subsystem. IDS performs unit and integration testing on all applications. All data within the application undergo validity and consistency checks as per the specifications. All specifications adhere to security and privacy regulations.

3.c. Is the data current? How do you know?
Yes. IDS requirements specify that data must be refreshed (re-extracted from Integrated Data Retrieval Systems (IDRS) or Corporate Files On-Line (CFOL) via SIA if the data is more than 48 hours old. This ensures that the data is accurate, timely, and complete before beginning analysis. Individual applications may also be programmed to automatically re-request data based on pre-determined criteria. Program requirements include checks and balances.

4. Are the data elements described in detail and documented? If yes, what is the name of the document?
The data elements are described and sources listed in the Software Requirements Specifications for the Inventory Delivery System (IDS). In addition, data elements are described in the Data Dictionary.

Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?

- Developers (IS Programmers and Analysts) through the use of live data waivers, have read only access.
- Systems Administrators administrate employee accounts. They do not have access to taxpayer accounts.
- Database Administrators have full access to all data.
- National Office Analyst in charge of the program have read only access
- Customer Service Representative (CSR) Managers-access to address and telephone number of the taxpayer
- Security Officer(s) has to send a request in order to have access to the data in the system.
- COTR has read only access
- TIGTA (Treasury Inspector General for Tax Administration) sends a request in order to have access to the data in the system.
- GAO (Government Accountability Office) – sends a request to local security and management is in charge of granting access to IDS data.

    - Audits must be incorporated in their plans, memos sent to IRS Executives indicating planned audit, scope of audit, etc. Forms 5081 (prepared and signed, and approved by appropriate levels) allowing access to the audited systems (access is never at the system administrator level)
- Contractors do not have access to IDS

2. How is access to the data by a user determined?
Access to data will be based on approved security rules determined by individual roles and responsibilities and will be restricted to a "need to know." Users will follow established IRS procedures for access using Online (OL) 5081 and rules described in Unauthorized Access (UNAX).

OL 5081 is used to document access requests, modifications, terminations for all types of users, including system administrators, system accounts requiring File Transfer Protocol (FTP) access, and test accounts. When a new user needs access to IRS systems or applications, the user's manager or designated official, accesses the Online 5081 (OL5081) application to request access for the new user. OL5081 is an online form, which includes information, such as the name of the system or application, type of access, and the manager's signature approving authorization of access. The completed OL5081 is submitted to the account administration approval group, who assigns a user ID and an initial password.

Before access is granted, the user is required to digitally sign OL5081 acknowledging his/her security responsibilities when using the system. The user signs security rules of behavior provided in the OL5081.

2. a. Are criteria, procedures, controls, and responsibilities regarding access documented?
Yes. All system access criteria, procedures and controls and responsibilities are detailed in the Solaris Administration Guide (SunOS 5.10 vol. 1 & 2), SunOS 5.10 User's Guide and Advanced User's Guide, Basic Security Module Guide (SunOS 5.10), Oracle Pro*C User's Guide, and the Trusted Facility Manual.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.
Access to data will be based on approved security rules determined by individual roles and responsibilities and will be restricted to a "need to know". Users will follow established IRS procedures for access using OL 5081 and rules described in UNAX.

4. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?
All IRS employees are required to abide by UNAX rules. In addition, the Restructuring and Reform Act of 1998 (RA98) and Privacy Act prohibit browsing by any employee. The Disclosure, Security and TIGTA offices assures compliance with the law by conducting annual reviews.

5.a Do other systems share data or have access to data in this system? If yes, explain.

Yes.

SIA provides entity and tax module data to IDS. IDS verifies the entity and tax module data and transfers the data back to IDS.

ICS sends a list of ZIP codes associated with business unit employees working a particular case.

TNR Vendor sends taxpayer telephone numbers to IDS. IDS verifies the taxpayer's telephone number and transfers the telephone numbers back to TNR.

ADR Vendor sends new taxpayer addresses and phone numbers to IDS and IDS verifies the taxpayer's address and phone numbers and sends the address and phone number back to ADR Vendor.

5.b. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?

The application analyst, security analyst, privacy analyst, and management.

6.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, & Other)?

Yes.

United States Postal Service sends IDS postal tracers (a yellow sticker attached to the return mail that displays the taxpayer's addresses.

Choicepoint sends third party data (e.g., taxpayer's addresses) to IDS

TIGTA and GAO will have access to the data upon written request.

6.b. How will the data be used by the agency?

TIGTA and GAO will use the data for auditing..

6.c. Who is responsible for assuring proper use of the data?
TIGTA and GAO are responsible for the security of the data and proper use of the data upon receipt.

6.d. How will the system ensure that agencies only get the information they are entitled to under IRC 6103?
TIGTA and GAO make their requests through the system's security staff. The system's security staff ensures that the request conforms with all laws and procedures including Internal Revenue Code (IRC) 6103.

Attributes of the Data

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes. The use of data is relevant and necessary for IDS to automate the scoring and routing processes. The system ensures that the address and/or telephone number is the most up-to-date available. By law, IRS needs to take certain steps to locate taxpayer's addresses/telephone numbers in order to pursue collection activities using the most cost-effective assignment of cases.

2.a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

Taxpayer: No. The system compiles existing data from various systems and passes recommendations to IDRS without affecting the original data or creating new taxpayer data.

Employee: No. The system compiles existing data from various systems and passes recommendations to IDRS without affecting the original data or creating new taxpayer data.

2.b. Will the new data be placed in the individual's record (taxpayer or employee)?

Taxpayer: No

Employee: No

2.c. Can the system make determinations about taxpayers or employees that would not be possible without the new data?

Taxpayer: N/A

Employee: N/A

2.d. How will the data be verified for relevance and accuracy?

N/A, IDS does not create new data.

3.a If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain.

Users will follow established IRS procedures for access using OL 5081 and rules described in UNAX.

3.b If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Users will follow established IRS procedures for access using OL 5081 and rules described in UNAX. In addition, annual security, disclosure, and TIGTA reviews will be conducted.

4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.

Yes. During reviews and testing, data can be retrieved by personal identifiers (TIN, file source, TIN Type, MFT, and Tax Period) through a database query. For testing purposes, a waiver was obtained to access live taxpayer data.

5. What are the potential effects on the due process rights of taxpayers and employees of:

a. Consolidation and linkage of files and systems:

Taxpayer: IDS automates the routing of the existing manual processes and does not change the current due process rights of taxpayers

Employee: IDS automates the routing of the existing manual processes and does not change the current due process rights of employees.

b. Derivation of data;

Taxpayer: N/A

Employee: N/A

c. Accelerated information processing and decision making;

Taxpayer: N/A

Employee: N/A

d. Use of new technologies;

No.

How are the effects to be mitigated?

There are no effects to be mitigated.

<u>Maintenance of Administrative Controls</u>

1.a. Explain how the system and its use will ensure equitable treatment of taxpayers and employees.

Treatment of taxpayers would be consistent nationwide. Except for variations in expenses based on census and demographic variations, all processes handle taxpayer records in the same fashion regardless of taxpayer's location. As an expert system, there are no processes that yield inconsistent taxpayer treatment across the country.

1.b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites?

The production system will be a consolidated site in Tennessee Computing Center (TCC). No other production sites will exist. The Western Development Center (WDC) is only in charge of development. All programs are controlled through ClearCase,(version control programs) and there is transmittal control of all software.

1.c. Explain any possibility of disparate treatment of individuals or groups.

No. IDS does not treat individuals or groups disparately**.** The system is designed to automate a current manual process, and use objective criteria to assign or close cases.

2.a. What are the retention periods of data in this system?

See attached data retention table.

2.b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

Data is deleted using an automated housekeeping routine (Records Disposition Handbook 1.15.2) when the last of the taxpayer's and related TINs cases have been processed/resolved. This application was developed for IDS according to security handbook 2.10 and uses required retentions periods.

2.c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

IDS requirements specify that data must be refreshed (re-extracted from IDRS or Corporate Files On-Line (CFOL) via SIA) if the data is more than 48 hours. This ensures that the data is accurate, timely, and complete before beginning analysis. Individual applications may also be programmed to automatically re-request data based on pre-determined criteria. Program requirements include checks and balances.

3.a Is the system using technologies in ways that the IRS has not previously employed (e.g. Caller-ID)?

This system does not use technologies in ways the IRS has not previously employed.

3.b How does the use of this technology affect taxpayer/employee privacy?

Taxpayer/employee privacy is maintained according to accepted security encryption procedures currently in place.

4.a Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes. The presence of taxpayer data with an individual identifier makes it possible to associate data with a given taxpayer. Also the system is able to locate new addresses, telephone numbers, and other third party data not currently shown on IDRS.

4.b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

Yes. IDS has the capability to query and group individuals.

4.c. What controls will be used to prevent unauthorized monitoring?

Access to data will be based on approved security rules determined by individual roles and responsibilities and will be restricted to a "need to know". Users will follow established IRS procedures for access using OL 5081 and rules described in UNAX. In addition to IRC section 6103 and IRS Code of Conduct.

5.a Under which Systems of Record Notice (SORN) does the system operate? Provide number and name.

System of Records Number(s) (SORN) #:
Treasury/IRS 23.012 Offers in Compromise
Treasury/IRS 26.016 Returns Compliance Program
Treasury/IRS 26.019 Taxpayer Delinquency Account
Treasury/IRS 26.020 Taxpayer Delinquency Investigation
Treasury/IRS 26.022 Delinquency Prevention Programs
Treasury/IRS 34.037 IRS Audit and Security Records System

5.b. If the system is being modified, will the SORN require amendment or revision? Explain
IDS is not being modified.

APPENDIX A – Data Retention Schedule

Data Type: Address Research Data
Retention Period: 12 months
Dating From ADR account creation

Data Type: Address History Data
Retention Period: 12 months
Dating From ADR account creation

Data Type: MIS results (Specific taxpayer case results)
Retention Period: No Limit
Dating From Completion of the related case

Data Type: MIS Reports
Retention Period: No Limit
Dating From Report creation date

Data Type: Self-Monitor Case Reports
Retention Period: No Limit
Dating From End of monitoring period

Data Type: Self-Monitor Lookup Data
Retention Period: 6 months
Dating From Completion of monitoring period

Data Type: TNR History Data
Retention Period: 24 months
Dating From Completion of the related case

Data Type: TNR IDRS upload data
Retention Period: 24 months
Dating From Completion of the related case

Data Type: TNR ACS upload data
Retention Period: 24 months
Dating From Completion of the related case

Data Type: All other IDS Account Data
Retention Period: 1 month
Dating From Date of account completion

Data Type: Cross Reference Case Data
Retention Period: 1 month
Dating From Date of account completion

Data Type: Input files from external sources
Retention Period: 3 months
Dating From Date file loaded onto IDS

Data Type: Output files to external systems
Retention Period: 3 months
Dating From Date file created on IDS

Data Type: Error Files
Retention Period: 3 months
Dating From Date file created on IDS

Data Type: Run Control Files
Retention Period: 3 months
Dating From Date file created on IDS

Data Type: Audit Trails
Retention Period: On-line 1 month; Off-line 7 years
Dating From Date file created on IDS

View other PIAs on IRS.gov